Office of the Designated Approving Authority (DAA)

A Year of Progress

ODAA Progress

(1) Implementing the ODAA Process

- Proof of Concept Validated!
- More IS Reps and ISSPs able to focus on on-site certifications, annual inspections and advice and assistance.
- Consistency in policy interpretation and plan development.
- Tracking of C&A cycle times.
- Roll Out ODAA Process in Three Phases.

ODAA Progress

Phase 1

- Technical Directors refocused and renamed as Regional DAAs (RDAA).
- Realigned ISSPs to ODAA.
- Only RDAAs issue accreditation letters.
- Consistent format on letters and process.
- All SSPs submitted electronically.
- Status: All completed

ODAA Progress

Phase 2

- All plans come into ODAA HQ for logging and provided back out to the Field for review by IS Rep and/or ISSPs.
- Once the plan is reviewed, the IS Rep or ISSP provides the draft accreditation letter to the RDAA just like in Phase 1.
- The difference in Phase 2 is that the ISSM submits the SSP directly to ODAA HQ for logging in the database.

ODAA Progress

Phase 3

- All plans come into ODAA HQ for logging and review.
- IS Reps and ISSPs no longer review plans.

- Status:
  - Currently, Four Field Offices and three large companies on West Coast and one large company in North East in Phase 3.
- Full Phase 3 implementation based on manpower at ODAA HQ.

ODAA Progress

(2) Expanded the use of Master System Security Plans (MSSPs)

- Broader MSSPs to be all encompassing.
- Specific details in the Protection Profiles.
  - Can’t be anything in the MSSP that contradicts what is in the Protection Profiles.
- Gives ISSMs self certification for “like” systems under an approved Protection Profile.
- Western contractor in large facility went from 13 MSSPs to 3.

ODAA Progress

(3) Issued the Cloning Procedure

- Provides additional efficiencies for the ISSMs.
- When used in accordance with the procedure, “like” systems can be added to an approved MSSP without the ISSM physically verifying every system.
- Without the Cloning procedure, the ISSM must verify (touch) every system configuration.
  - Risk management decision to speed up the process.

ODAA Progress

(4) Fluid IATOs

- Systems under an IATO can be modified by the contractor to meet changing mission demands without requiring the issuance of a new IATO
  - DAA must be given prior notification and approval.
- System frozen (no changes allowed) a week prior to the scheduled on-site inspection so the system will match the approved plan used by the ISSP for the inspection.

ODAA Progress

(5) Revised the Policy Interpretation on ISSMs

- A Primary and Alternate ISSM may be assigned to the same Cage Code and may operate with the same authority and without restrictions.
- Allows two ISSMs to support a Cage Code simultaneously, which is a change from past policy interpretations that only allowed the Alternate to operate in the absence of the Primary.
- Subordinate ISSMs may be assigned to support large facilities but the Primary ISSM is still held accountable.

ODAA Progress

(6) Clarified the definition of Security Relevant changes that would require reaccreditation

- Security relevance focused primarily on anything that impacts identification, authorization, and auditing.
- Most changes can be a pen and ink change and not require reaccreditation.

ODAA Progress

(7) NISP and Audit Tools posted

- Tests the secure configuration of certain systems and reduces the number of auditable items and the resulting log files.
- Not mandatory.

ODAA Progress

(8) Limited 90 day ATOs for SIPRNET

- DISA agreed to accept limited 90 day ATOs from DSS.
- Allows contractors SIPRNET access while purchasing and installing the required Firewall and Intrusion Detection Systems (IDS).

Path Forward

Continuing Challenges for DSS

- Bring all Field Offices to Phase 3
- Revise, update and issue ISOM Chapter 10
- Continue to address and resolve issues that have latitude for policy implementation.

Path Forward

Continuing Challenges for Industry

- Hire ISSMs that are policy knowledgeable to write NISPOM compliant security plans.
  - 63% failure rate on SSP received from ISSM
- Hire ISSM that are technically knowledgeable to maintain the secure configurations as identified in the SSPs.
  - Most systems are not configured correctly prior to the DSS on-site validation.
- Continue to support dialog on issues.